(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－353226
（P2000－353226A）
(43)公開日　平成12年12月19日(2000.12.19)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｋ 19/07		Ｃ０６Ｋ 19/00	Ｎ	
17/00		17/00	Ｄ	
19/00		Ｇ０９Ｃ 1/00	６６０Ｄ	
Ｇ０９Ｃ 1/00	６６０	Ｇ０６Ｋ 19/00	Ｑ	
Ｇ１０Ｌ 19/00		Ｃ１０Ｌ 9/00	Ｎ	

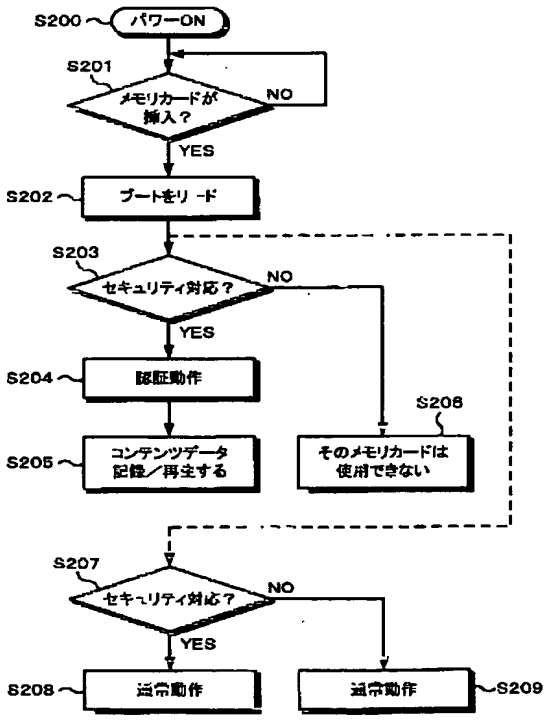
審査請求　未請求　請求項の数７　ＯＬ　（全 18 頁）　最終頁に続く

(21)出願番号　特願2000－105007(P2000－105007)
(22)出願日　平成12年４月６日(2000.4.6)
(31)優先権主張番号　特願平11－99948
(32)優先日　平成11年４月７日(1999.4.7)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　岡上　拓己
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　佐々　哲
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100082762
弁理士　杉浦　正知

(54)【発明の名称】　メモリ装置、データ処理装置および方法

(57)【要約】
【課題】　セキュリティ機能のような新機能をメモリ装置が持つかどうかを瞬時に決定する。
【解決手段】　機器の電源がオンされると、メモリカードが挿入されているかどうかが決定され、メモリカード中のブートブロックが読み込まれる（ステップＳ２０２）。ブートブロック中の識別情報を参照して、挿入されたメモリカードがセキュリティ対応か、非対応かが決定される（ステップＳ２０３）。セキュリティ対応のメモリカードであれば、認証動作がなされ（ステップＳ２０４）、認証成立後にコンテンツデータの記録／再生がなされる（ステップＳ２０５）。セキュリティ非対応のメモリカードの場合には、ステップＳ２０６において、そのメモリカードが使用できない旨の告知がなされる。若し、機器がセキュリティ非対応の場合には、ステップＳ２０７における決定の結果が肯定、否定の何れであっても、ステップＳ２０８およびＳ２０９で示すように、メモリカードに対して、通常動作を行う。



【特許請求の範囲】
【請求項１】　データ処理装置に対して着脱自在のメモリ装置において、
不揮発性メモリと、
既存のメモリ装置と異なる新機能を実現するための手段と、
データ処理装置と上記不揮発性メモリとの間に配されたインタフェース手段とを備え、
上記不揮発性メモリの記憶領域中で、使用時にデータ処理装置によって最初に読まれる所定の記憶領域に、上記新機能を持つかどうかの識別情報を記録することを特徴とするメモリ装置。
【請求項２】　着脱自在で、不揮発性メモリを含むメモリ装置を記録媒体として使用するデータ処理装置において、
メモリ装置と通信を行うインタフェース手段と、
既存のメモリ装置を使用した場合と異なる新機能を実現するための手段とを備え、
上記メモリ装置を使用する時に、最初に読み込む所定の記憶領域中の識別情報によって、装着されたメモリ装置が上記新機能を有するかどうかを決定するようにしたデータ処理装置。
【請求項３】　請求項１または２において、
上記新機能がセキュリティ機能であることを特徴とするメモリ装置。
【請求項４】　データ処理装置によって、データ処理装置に対して着脱自在のメモリ装置に対して情報の書き込みまたは読み出しを行うデータ処理方法において、
メモリ装置を使用する時に、最初に上記メモリ装置内の不揮発性メモリの所定の記憶領域を読み出すステップと、
上記記憶領域中の識別情報によって、既存のメモリ装置と異なる新機能を上記メモリ装置が有するか否かを決定するステップとからなることを特徴とするデータ処理方法。
【請求項５】　請求項４において、
上記新機能がセキュリティ機能であることを特徴とするデータ処理方法。
【請求項６】　請求項４において、
データ処理装置が上記新機能に対応している時に、
上記メモリ装置が上記新機能を有すると決定される場合に、データの書き込みまたは読み出しを行い、上記メモリ装置が上記新機能を有しないと決定される場合に、データの書き込みまたは読み出しを行わないステップをさらに有することを特徴とするデータ処理方法。
【請求項７】　請求項４において、
データ処理装置が上記新機能に対応していない時に、
上記メモリ装置が上記新機能を有する否かに係わらず、データの書き込みまたは読み出しを行うステップをさらに有することを特徴とするデータ処理方法。

【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は、例えばオーディオデータを記録する媒体として、機器に着脱自在のメモリカードを使用するようにしたメモリ装置、データ処理装置および方法に関する。
【０００２】
【従来の技術】ＥＥＰＲＯＭ(Electrically Erasable Programmable ROM)と呼ばれる電気的に書き換え可能な不揮発性メモリは、１ビットを２個のトランジスタで構成するために、１ビット当たりの占有面積が大きく、集積度を高くするのに限界があった。この問題を解決するために、全ビット一括消去方式により１ビットを１トランジスタで実現することが可能なフラッシュメモリが開発された。フラッシュメモリは、磁気ディスク、光ディスク等の記録媒体に代わりうるものとして期待されている。
【０００３】フラッシュメモリを機器に対して着脱自在に構成したメモリカードも知られている。このメモリカードを使用すれば、従来のＣＤ（コンパクトディスク）、ＭＤ（ミニディスク）等のディスク状媒体に代えてメモリカードを使用するディジタルオーディオ記録／再生装置を実現することができる。
【０００４】メモリカードを記録媒体とするオーディオレコーダでは、ディジタル記録／再生を行うので、比較的高品質のデータを復元できる圧縮方式を使用している場合には、記録／再生される曲等の著作権を保護する必要がある。その方法の一つとして、暗号化技術によって、真正なメモリカード以外のメモリカードを使用不可能とする方法がある。すなわち、真正なレコーダと真正なメモリカードの組み合わせによって、暗号化を復号化することを可能とするものである。また、著作権保護に限らず、メモリカードに格納された情報の機密性が必要なために暗号化技術を採用する場合もある。
【０００５】従来のメモリカードは、それ自体に暗号化の機能を持っていなかった。従って、機密性の必要なデータをメモリカードに記録しようとする場合、セット側においてデータを暗号化し、暗号化されたデータをメモリカードに記録することが必要とされる。しかしながら、復号化のキーをメモリカード上に格納する場合には、機密性が保たれない。一方、復号化のキーをセット内にとどめた場合には、暗号化されたデータをそのセット以外に復号化することができず、メモリカードの互換性を保てない問題がある。例えば自分のセットで記録したメモリカードを他人のセットでは、復号できない。この問題を解決するために、セットおよびメモリカードの両者が暗号化の機能を持ち、相互認証を行うことによって、機密性とカードの互換性を確保することが提案されている。
【０００６】実際には、著作権保護が不要なデータをメ

モリカードに記録／再生することがある。例えば会話を記録するような場合には、オーディオ圧縮方式としては、復元される音声の品質が比較的悪くても、圧縮率が高いものが使用される。この場合には、著作権保護は、不要である。また、電子スチルカメラ、ビデオカメラ等で撮影した画像を記録する媒体としてメモリカードを使用する場合も、著作権保護が不要である。一般的に暗号化の機能を持つ、セキュリティ対応のメモリカードは、それを持たないメモリカード、すなわち、従来型のメモリカードに比してコストが高く、高価なものとなる。従って、著作権保護、機密性の保持の必要性に応じて、セキュリティ対応のメモリカードと、非対応のメモリカードを利用することが予想される。

【０００７】セットおよびメモリカードがそれぞれセキュリティ対応と、非対応の２種類存在する場合、まず、セキュリティ機能を動作させ、正常な動作がなされるか、エラーになるのかによって、セキュリティ対応、セキュリティ非対応を決定する必要があった。他の方法では、メモリカードの形状を機能の相違に応じて異ならせるようになされる。例えば切欠の有無で区別し、セキュリティ機能を有するメモリカードは、セキュリティ非対応のメモリカードを使用する下位の機器に装着不可能とするようになされる。

【０００８】

【発明が解決しようとする課題】セキュリティ機能を持つかどうかを決定する時に、セキュリティ機能を実際に動作させる方法は、エラーとなる場合には、その動作が無駄となり、また、無駄な動作により遅延が生じ、利用者にとって快適な操作環境とはいえない問題がある。また、形状で区別する方法は、機器とメモリカードの対応関係が一義的に決まってしまい、例えばセキュリティ機能を有するメモリカードを、セキュリティ機能が発揮されないけれども、下位の機器で使用する可能性をなくしてしまう問題がある。すなわち、セキュリティ非対応のセットが既に存在している場合には、既存のセットによってセキュリティ対応のメモリカードを使用できることが望まれる。例えば、セキュリティ非対応のハンディームービー（カメラ一体型の記録再生機）が撮影した画像をセキュリティ対応のメモリカードに記録し、メモリカードから再生できることが望まれる。この場合には、暗号化の機能が使用されない。

【０００９】従って、この発明の目的は、上述した問題を生じることなく、メモリ装置が既存のものとは異なる新機能を持つかどうかを決定することができるメモリ装置、データ処理装置および方法を提供することにある。

【００１０】

【課題を解決するための手段】上述した課題を解決するために、請求項１の発明は、データ処理装置に対して着脱自在のメモリ装置において、不揮発性メモリと、既存のメモリ装置と異なる新機能を実現するための手段と、データ処理装置と不揮発性メモリとの間に配されたインタフェース手段とを備え、不揮発性メモリの記憶領域中で、使用時にデータ処理装置によって最初に読まれる所定の記憶領域に、新機能を持つかどうかの識別情報を記録することを特徴とするメモリ装置である。

【００１１】請求項２の発明は、着脱自在で、不揮発性メモリを含むメモリ装置を記録媒体として使用するデータ処理装置において、メモリ装置と通信を行うインタフェース手段と、既存のメモリ装置を使用した場合と異なる新機能を実現するための手段とを備え、メモリ装置を使用する時に、最初に読み込む所定の記憶領域中の識別情報によって、装着されたメモリ装置が新機能を有するかどうかを決定するようにしたデータ処理装置である。

【００１２】請求項４の発明は、データ処理装置によって、データ処理装置に対して着脱自在のメモリ装置に対して情報の書き込みまたは読み出しを行うデータ処理方法において、メモリ装置を使用する時に、最初にメモリ装置内の不揮発性メモリの所定の記憶領域を読み出すステップと、記憶領域中の識別情報によって、既存のメモリ装置と異なる新機能をメモリ装置が有するか否かを決定するステップとからなることを特徴とするデータ処理方法である。

【００１３】この発明では、メモリ装置を使用する時に、最初に読み出される不揮発性メモリの領域に、新機能を持つかどうかの識別情報を記録する。データ処理装置は、この識別情報から直ちにメモリ装置が新機能を持つかどうかを設定することができる。

【００１４】

【発明の実施の形態】以下、この発明の一実施形態について説明する。図１は、この発明の一実施形態の全体の構成を示す。この一実施形態は、記録媒体として、着脱自在のメモリカードを使用するディジタルオーディオ信号のレコーダ（記録および再生機）である。図１において、破線が囲んで示す１がセットとしてのレコーダを示し、４０がレコーダに着脱自在のメモリカードを示す。なお、この発明は、ディジタルオーディオ信号以外に動画データ、静止画データ等の記録／再生に対しても適用できる。

【００１５】レコーダ１は、ＣＰＵ２と、ＣＰＵ２とバスで接続されたセキュリティブロックと、操作ボタン４と、表示デバイス５とを有している。セキュリティブロック３は、ＤＥＳ(Data Encryption Standard)の暗号化回路を含む。操作ボタン４からのユーザの操作に応じて発生した録音指令、再生指令等のデータがバスを介してＣＰＵ２に与えられる。種々の情報、レコーダ１の動作状態等が表示デバイス５によって表示される。さらに、６は、外部入出力と内部のオーディオエンコーダ／デコーダ７との間に設けられたオーディオインターフェースである。

【００１６】後述するように、メモリカード４０は、フ

ラッシュメモリ（不揮発性メモリ）４２、ＤＥＳの暗号化回路を含むセキュリティブロック５２、通信用インターフェース、レジスタ等が１チップ上にＩＣ化されたものである。メモリカード４０は、レコーダ１に対して着脱自在とされている。なお、この一実施形態では、暗号化機能を有しないメモリカード、すなわち、セキュリティブロックを有しないメモリカードをレコーダ１が使用することが可能とされている。

【００１７】オーディオエンコーダ／デコーダ7は、ディジタルオーディオ信号を高能率符号化し、また、高能率符号化データを復号する。高能率符号化方法としては、ミニディスクで採用されているＡＴＲＡＣ(Adaptive Transform Acoustic Coding)を改良したもの（ＡＴＲＡＣ３と表記する）が使用できる。ＡＴＲＡＣ３では、４４．１kHzでサンプリングした１サンプル１６ビットのオーディオデータを処理する。ＡＴＲＡＣ３でオーディオデータを処理する時の最小のデータ単位がサウンドユニットＳＵである。１ＳＵは、１０２４サンプル分（１０２４×１６ビット×２チャンネル）を数百バイトに圧縮したものであり、時間にして約２．３m秒である。ＡＴＲＡＣ３により約１／１０にオーディオデータが圧縮される。ミニディスクにおいてそうであるように、ＡＴＲＡＣ３の工夫された信号処理によって、圧縮／伸長処理による音質の劣化は少ない。

【００１８】ＭＤ（ミニディスク）の再生出力、チューナの出力、テープ再生出力等のアナログオーディオ信号８がＡ／Ｄ変換器９によりディジタルオーディオ信号へ変換され、ディジタルオーディオ信号がオーディオインターフェース６に供給される。ディジタル入力１０は、ＭＤまたはＣＤ（コンパクトディスク）の再生出力、ディジタル放送、ネットワークで配信されたオーディオデータ等である。ディジタル入力１０がオーディオインターフェース６に供給される。ディジタル入力１０は、例えば光ケーブルを介して伝送される。オーディオインターフェース６では、入力選択の処理がされ、選択された入力ディジタルオーディオ信号がオーディオエンコーダ／デコーダ７に供給される。

【００１９】オーディオエンコーダ／デコーダ７からの符号化データがセキュリティブロック３において暗号化される。セキュリティブロック３は、コンテンツ（ここでは、ディジタルオーディオ信号）の著作権を保護するための備えられている。レコーダ１のセキュリティブロック３は、複数のマスターキーと機器毎にユニークなストレージキーを持つ。さらに、乱数発生回路を持ち、セキュリティブロック５２を内蔵するメモリカード４０が装着された時に、装着されたものが真正なものであるかを確認する認証を行い、正しく認証できれば、セッションキーを共有することができる。

【００２０】セキュリティブロック３からの暗号化されたオーディオデータがＣＰＵ２に供給される。ＣＰＵ２は、着脱機構（図示しない）に装着されたメモリカード４０とメモリインタフェース１１を介しての通信を行い、暗号化されたデータをメモリカード４０のフラッシュメモリ４２に書き込む。メモリインタフェース１１によって、ＣＰＵ２とメモリカード４０との間では、シリアル通信がなされる。

【００２１】ＣＰＵ２およびメモリインタフェース１１によってメモリカード４０から読み出した暗号化されたオーディオデータは、セキュリティブロック３によって復号化され、オーディオエンコーダ／デコーダ７によって復号化処理を受ける。オーディオエンコーダ／デコーダ７の出力がオーディオインターフェース６を介してＤ／Ａ変換器１２に供給され、アナログオーディオ出力１３へ変換される。また、オーディオエンコーダ／デコーダ７からのオーディオデータ、並びにセキュリティブロック３からの復号化データがインターフェース６を介してディジタル出力１４および１５として出力される。

【００２２】図２は、メモリカード４０の構成を示す。メモリカード４０は、コントロールブロック４１とフラッシュメモリ４２が１チップＩＣとして構成されたものである。レコーダ１のＣＰＵ２とメモリカード４０との間の双方向シリアルインタフェース（メモリインタフェース１１）は、１０本の線からなる。主要な４本の線は、データ伝送時にクロックを伝送するためのクロック線ＳＣＫと、ステータスを伝送するためのステータス線ＳＢＳと、データを伝送するデータ線ＤＩＯ、インターラプト線ＩＮＴとである。その他に電源供給用線として、２本のＧＮＤ線および２本のＶＣＣ線が設けられる。２本の線Ｒｅｓｅｒｖは、未定義の線である。

【００２３】クロック線ＳＣＫは、データに同期したクロックを伝送するための線である。ステータス線ＳＢＳは、メモリカード４０のステータスを表す信号を伝送するための線である。データ線ＤＩＯは、コマンドおよび暗号化されたオーディオデータを入出力するための線である。インターラプト線ＩＮＴは、メモリカード４０からレコーダ１のＣＰＵ２に対しての割り込みを要求するインターラプト信号を伝送する線である。メモリカード４０を装着した時にインターラプト信号が発生する。但し、この一実施形態では、かかるインターラプト信号をデータ線ＤＩＯを介して伝送するようにしているので、インターラプト線ＩＮＴを接地し、使用していない。

【００２４】コントロールブロック４１のシリアル／パラレル変換・パラレル／シリアル変換・インタフェースブロック（Ｓ／Ｐ，Ｐ／Ｓ，ＩＦブロックと略す）４３は、上述した複数の線を介して接続されたレコーダ１のメモリインタフェース１１とコントロールブロック４１とのインタフェースである。Ｓ／Ｐ，Ｐ／Ｓ，ＩＦブロック４３は、レコーダ１から受け取ったシリアルデータをパラレルデータに変換し、コントロールブロック４１に取り込み、コントロールブロック４１からのパラレル

データをシリアルデータに変換してレコーダ１に送る。また、S／P，P／S，IFブロック４３は、データ線DIOを介して伝送されるコマンドおよびデータを受け取った時に、フラッシュメモリ４２に対する通常のアクセスのためのコマンドおよびデータと、暗号化に必要なコマンドおよびデータとを分離する。

【００２５】つまり、データ線DIOを介して伝送されるフォーマットでは、最初にコマンドが伝送され、その後にデータが伝送される。S／P，P／S，IFブロック４３は、コマンドのコードを見て、通常のアクセスに必要なコマンドおよびデータか、暗号化に必要なコマンドおよびデータかを判別する。この判別結果に従って、通常のアクセスに必要なコマンドをコマンドレジスタ４４に格納し、データをページバッファ４５およびライトレジスタ４６に格納する。ライトレジスタ４６と関連してエラー訂正符号化回路４７が設けられている。ページバッファ４５に一時的に蓄えられたデータに対して、エラー訂正符号化回路４７がエラー訂正符号の冗長コードを生成する。

【００２６】コマンドレジスタ４４、ページバッファ４５、ライトレジスタ４６およびエラー訂正符号化回路４７の出力データがフラッシュメモリインタフェースおよびシーケンサ（メモリI／F，シーケンサと略す）５１に供給される。メモリIF，シーケンサ５１は、コントロールブロック４１とフラッシュメモリ４２とのインタフェースであり、両者の間のデータのやり取りを制御する。メモリIF，シーケンサ５１を介してデータがフラッシュメモリ４２に書き込まれる。

【００２７】フラッシュメモリ４２から読み出されたデータがメモリIF，シーケンサ５１を介してページバッファ４５、リードレジスタ４８、エラー訂正回路４９に供給される。ページバッファ４５に記憶されたデータがエラー訂正回路４９によってエラー訂正がなされる。エラー訂正がされたページバッファ４５の出力およびリードレジスタ４８の出力がS／P，P／S，IFブロック４３に供給され、上述したシリアルインタフェースを介してレコーダ１のCPU２に供給される。

【００２８】著作権保護のために、レコーダ１のセキュリティIC４０とメモリカード４０のセキュリティブロック５２とによって、フラッシュメモリ４２に書き込まれるコンテンツ（ATRAC３により圧縮されたオーディオデータ、以下ATRAC３データと表記する）は、暗号化される。セキュリティブロック５２は、バッファメモリ５３、DESの暗号化回路５４、不揮発性メモリ５５等を有する。

【００２９】なお、５０は、メモリカード４０のバージョン情報、各種の属性情報等が格納されているコンフィグレーションROMである。また、メモリカード４０には、ユーザが必要に応じて操作可能な誤消去防止用のスイッチ６０が備えられている。このスイッチ６０が消去禁止の接続状態にある場合には、フラッシュメモリ４２を消去することを指示するコマンドがレコーダ１側から送られてきても、フラッシュメモリ４２の消去が禁止される。さらに、６１は、メモリカード４０の処理のタイミング基準となるクロックを発生する発振器である。

【００３０】メモリカード４０のセキュリティブロック５２は、複数の認証キーとメモリカード毎にユニークなストレージキーを持つ。不揮発性メモリ５５は、暗号化に必要なキーを格納するもので、外部からは見えない。例えばストレージキーが不揮発性メモリ５５に格納される。さらに、乱数発生回路を持ち、専用（ある決められたデータフォーマット等の使用が同じシステム内の意味）レコーダ１と正しく認証ができ、セッションキーを共有できる。ATRAC３データを暗号化するためのコンテンツキーは、セッションキーで暗号化されてレコーダ１とメモリカード４０との間で伝送される。メモリカード４０のセキュリティブロック５２と同様に、レコーダ１のセキュリティブロック３もセット固有のストレージキーを有する。暗号化されたコンテンツを移動する時に、ストレージキーを使用してコンテンツキーが掛け直される。

【００３１】図３は、暗号化機能を有しない（すなわち、セキュリティ非対応）メモリカード４０’を示す。図２に示し、上述したメモリカード４０と比較すると、S／P，P／S，IFブロック４３に対して、セキュリティブロック５２が接続されていない。その他の構成に関して、メモリカード４０と４０’とは同一である。また、形状、サイズもメモリカード４０と４０’とが同一とされている。図１に示すレコーダ１は、セキュリティ対応のものであるので、メモリカードとの相互認証、キーの通信等を行う。若し、セキュリティに対応していない図３に示すメモリカード４０’を装着すると、レコーダ１は、メモリカード４０’がセキュリティ非対応のもので、メモリカード４０’を使用できないものと決定する。

【００３２】レコーダ１がメモリカードの種類を決定する方法としては、幾つかのものを利用できる。一つの方法では、メモリカードを装着した時に、認証を行うために、キーを伝送する時に、メモリカード４０’からは、正規の応答を受信できず、レコーダ１においてタイムアウトの決定がされ、その結果、メモリカードがセキュリティ非対応のものと決定できる。他の方法では、メモリカードを装着した時に、最初にレコーダ１に読み込まれるメモリカードの領域（ブート領域）中に、セキュリティ対応／非対応の識別情報を記録しておき、この識別情報に基づいてレコーダ１がメモリカードの種類を決定することができる。

【００３３】また、図１に示すレコーダ１に限らず、セキュリティ非対応のメモリカード４０’を使用するようにした機器も存在する。例えばCCDカメラで撮影した

画像をメモリカードに記録し、メモリカードから撮影画像を再生する機能を有する、ディジタルハンディムービーは、メモリカード４０’を使用できる。かかるディジタルハンディムービーは、セキュリティ対応のメモリカード４０を使用できないのが普通である。後述するように、この発明の一実施形態では、メモリカード４０の互換性を高めるために、セキュリティ非対応のディジタルハンディムービーのようなセットがメモリカード４０を使用した記録および再生ができるように、メモリカード４０が構成されている。すなわち、上述したように、Ｓ／Ｐ，Ｐ／Ｓ，ＩＦブロック４３は、フラッシュメモリ４２に対して書き込み／読み出し用のコマンドおよびデータと、セキュリティブロックに必要なコマンドおよびデータとを分離する機能を有している。

【００３４】上述したこの発明の一実施形態についてさらに詳細に説明する。図４は、メモリカードを記憶媒体とするコンピュータシステムのファイルシステム処理階層を示す。ファイルシステム処理階層としては、アプリケーション処理層が最上位であり、その下に、ファイル管理処理層、論理アドレス管理層、物理アドレス管理層、フラッシュメモリアクセスが順次おかれる。この階層構造において、ファイル管理処理層がＦＡＴファイルシステムである。物理アドレスは、フラッシュメモリの各ブロックに対して付されたもので、ブロックと物理アドレスの対応関係は、不変である。論理アドレスは、ファイル管理処理層が論理的に扱うアドレスである。

【００３５】図５は、メモリカード４０におけるフラッシュメモリ４２のデータの物理的構成の一例を示す。フラッシュメモリ４２は、セグメントと称されるデータ単位が所定数のブロック（固定長）へ分割され、１ブロックが所定数のページ（固定長）へ分割される。フラッシュメモリ４２では、ブロック単位で消去が一括して行われ、書き込みと読み出しは、ページ単位で一括して行われる。各ブロックおよび各ページは、それぞれ同一のサイズとされ、１ブロックがページ０からページｍで構成される。１ブロックは、例えば８ＫＢ（Ｋバイト）バイトまたは１６ＫＢの容量とされ、１ページが５１２Ｂの容量とされる。フラッシュメモリ４２全体では、１ブロック＝８ＫＢの場合で、４ＭＢ（５１２ブロック）、８ＭＢ（１０２４ブロック）とされ、１ブロック＝１６ＫＢの場合で、１６ＭＢ（１０２４ブロック）、３２ＭＢ（２０４８ブロック）、６４ＭＢ（４０９６ブロック）の容量とされる。

【００３６】１ページは、５１２バイトのデータ部と１６バイトの冗長部とからなる。冗長部の先頭の３バイトは、データの更新に応じて書き換えられるオーバーライト部分とされる。３バイトの各バイトに、先頭から順にブロックステータス、ページステータス、更新ステータスが記録される。冗長部の残りの１３バイトの内容は、原則的にデータ部の内容に応じて固定とされる。１３バイトは、管理フラグ（１バイト）、論理アドレス（２バイト）、フォーマットリザーブの領域（５バイト）、分散情報ＥＣＣ（２バイト）およびデータＥＣＣ（３バイト）からなる。分散情報ＥＣＣは、管理フラグ、論理アドレス、フォーマットリザーブに対する誤り訂正用の冗長データであり、データＥＣＣは、５１２バイトのデータに対する誤り訂正用の冗長データである。

【００３７】管理フラグとして、システムフラグ（その値が１：ユーザブロック、０：ブートブロック）、変換テーブルフラグ（１：無効、０：テーブルブロック）、コピー禁止指定（１：ＯＫ、０：ＮＧ）、アクセス許可（１：ｆｒｅｅ、０：リードプロテクト）の各フラグが記録される。

【００３８】先頭の二つのブロック０およびブロック１がブートブロックである。ブロック１は、ブロック０と同一のデータが書かれるバックアップ用である。ブートブロックは、カード内の有効なブロックの先頭ブロックであり、メモリカードを機器に装填した時に最初にアクセスされるブロックである。残りのブロックがユーザブロックである。ブートブロックの先頭のページ０にヘッダ、システムエントリ、ブート＆アトリビュート情報が格納される。ページ１に使用禁止ブロックデータが格納される。ページ２にＣＩＳ(Card Information Structure)／ＩＤＩ(Identify Drive Information)が格納される。

【００３９】図６は、ブートブロックのフォーマットを示す。ブートブロックのヘッダ（３６８バイト）には、ブートブロックＩＤ、フォーマットバージョン、ブートブロック内の有効なエントリ数が記録される。システムエントリ（４８バイト）には、使用禁止ブロックデータの開始位置、そのデータサイズ、データ種別、ＣＩＳ／ＩＤＩのデータ開始位置、そのデータサイズ、データ種別が記録される。

【００４０】図７は、ブート＆アトリビュート情報（９６８バイト）を詳細に示す。ブート＆アトリビュート情報には、メモリカードのクラス、タイプ（読み出し専用、リードおよびライト可能、両タイプのハイブリッド等）、ブロックサイズ、ブロック数、総ブロック数、セキュリティ対応か否か、カードの製造に関連したデータ（製造年月日等）等が記録される。セットは、このセキュリティ対応か否かの識別情報（１バイト）によって、装着されたメモリカードがセキュリティ対応か否かを決定できる。図７において、（＊１）が付された情報は、セット側が読み出して装着時に確認する項目であり、（＊２）が付された情報は、製造および品質管理上の情報を設定する項目である。

【００４１】フラッシュメモリは、データの書き換えを行うことにより絶縁膜の劣化を生じ、書き換え回数が制限される。従って、ある同一の記憶領域（ブロック）に対して繰り返し集中的にアクセスがなされることを防止

する必要がある。従って、ある物理アドレスに格納されているある論理アドレスのデータを書き換える場合、フラッシュメモリのファイルシステムでは、同一のブロックに対して更新したデータを再度書き込むことはせずに、未使用のブロックに対して更新したデータを書き込むようになされる。その結果、データ更新前における論理アドレスと物理アドレスの対応関係が更新後では、変化する。このような処理（スワップ処理と称する）を行うことで、同一のブロックに対して繰り返して集中的にアクセスがされることが防止され、フラッシュメモリの寿命を延ばすことが可能となる。

【００４２】論理アドレスは、一旦ブロックに対して書き込まれたデータに付随するので、更新前のデータと更新後のデータの書き込まれるブロックが移動しても、ＦＡＴからは、同一のアドレスが見えることになり、以降のアクセスを適正に行うことができる。スワップ処理により論理アドレスと物理アドレスとの対応関係が変化するので、両者の対応を示す論理－物理アドレス変換テーブルが必要となる。このテーブルを参照することによって、ＦＡＴが指定した論理アドレスに対応する物理アドレスが特定され、特定された物理アドレスが示すブロックに対するアクセスが可能となる。

【００４３】論理－物理アドレス変換テーブルは、ＣＰＵ２によってメモリ上に格納される。若し、ＲＡＭ容量が少ない時は、フラッシュメモリ中に格納することができる。このテーブルは、概略的には、昇順に並べた論理アドレス（２バイト）に物理アドレス（２バイト）をそれぞれ対応させたテーブルである。フラッシュメモリの最大容量を１２８ＭＢ（８１９２ブロック）としているので、２バイトによって８１９２のアドレスを表すことができる。また、論理－物理アドレス変換テーブルは、セグメント毎に管理され、そのサイズは、フラッシュメモリの容量に応じて大きくなる。例えばフラッシュメモリの容量が８ＭＢ（２セグメント）の場合では、２個のセグメントのそれぞれに対して２ページが論理－物理アドレス変換テーブル用に使用される。論理－物理アドレス変換テーブルを、フラッシュメモリ中に格納する時には、上述した各ページの冗長部における管理フラグの所定の１ビットによって、当該ブロックが論理－物理アドレス変換テーブルが格納されているブロックか否かが指示される。

【００４４】上述したメモリカードは、ディスク状記録媒体と同様にパーソナルコンピュータのＦＡＴファイルシステムによって使用可能なものである。図５には示されてないが、フラッシュメモリ上にＩＰＬ領域、ＦＡＴ領域およびルート・ディレクトリ領域が設けられる。ＩＰＬ領域には、最初にレコーダのメモリにロードすべきプログラムが書かれているアドレス、並びにメモリの各種情報が書かれている。ＦＡＴ領域には、ブロック（クラスタ）の関連事項が書かれている。ＦＡＴには、未使用のブロック、次のブロック番号、不良ブロック、最後のブロックをそれぞれ示す値が規定される。さらに、ルートディレクトリ領域には、ディレクトリエントリ（ファイル属性、更新年月日、開始クラスタ、ファイルサイズ等）が書かれている。

【００４５】さらに、この一実施形態では、上述したメモリカード４０のフォーマットで規定されるファイル管理システムとは別個に、音楽用ファイルに対して、ファイル管理情報（トラック情報管理ファイル）を規定している。トラック情報管理ファイルは、メモリカード４０のユーザブロックを利用してフラッシュメモリ４２上に記録される。それによって、メモリカード４０上のＦＡＴが壊れても、ファイルの修復を可能とできる。

【００４６】トラック情報管理ファイルは、ＣＰＵ２により作成される。例えば最初に電源をオンした時に、メモリカード４０が装着されているか否かが判定され、メモリカードが装着されている時には、フラッシュメモリ４２のブートブロックがＣＰＵ２に読み込まれる。ブートブロック中の識別情報によって、装着したメモリカードがセキュリティ対応か、非対応かが決定される。セキュリティ対応であると決定されると、認証動作がなされる。その他のメモリカード４０から読み込まれたデータは、ＣＰＵ２が管理するメモリ（図示せず）に格納される。ユーザが購入して初めて使用するメモリカードでも、出荷時にフラッシュメモリ４２には、ＦＡＴや、ルートディレクトリの書き込みがなされている。トラック情報管理ファイルは、録音がなされると、作成される。認証が成立すると、レコーダ１によって、暗号化されたＡＴＲＡＣ３データファイルが記録／再生される。

【００４７】記録時には、操作ボタン４で録音ボタンを押すことによって発生した録音指令がＣＰＵ２に与えられる。そして、入力したオーディオデータがエンコーダ／デコーダ７によって圧縮され、エンコーダ／デコーダ７からのＡＴＲＡＣ３データがセキュリティブロック３により暗号化される。ＣＰＵ２が暗号化されたＡＴＲＡＣ３データをメモリカード４０のフラッシュメモリ４２に記録する。この記録後にＦＡＴおよびトラック情報管理ファイルが更新される。ファイルの更新の度、具体的には、オーディオデータの記録を開始し、記録を終了する度に、ＣＰＵ２が制御するメモリ（図示せず）上でＦＡＴおよびトラック情報管理ファイルが書き換えられる。そして、メモリカード４０を外す時に、またはパワーをオフする時に、メモリからメモリカード４０のフラッシュメモリ４２上に最終的なＦＡＴおよびトラック情報管理ファイルが格納される。この場合、オーディオデータの記録を開始し、記録を終了する度に、フラッシュメモリ４２上のＦＡＴおよびトラック情報管理ファイルを書き換えても良い。編集を行った場合も、トラック情報管理ファイルの内容が更新される。

【００４８】上述したこの発明の一実施形態におけるセ

キュリティ保護機能についてさらに説明する。最初に図８を参照してコンテンツにおけるキーの関係について説明する。メモリカード４０のフラッシュメモリ４２上では、図８Ａに示すように、キーエリア１０１が設けられ、キーエリア１０１にコンテンツ（暗号化されたオーディオデータのトラック（曲））毎に作成されるコンテンツキーＣＫがメモリカードに固有のストレージキーＫｓｔｍで暗号化されて格納されている。暗号化は、ＤＥＳと表記され、コンテンツキーＣＫをストレージキーＫｓｔｍで暗号化した場合には、ＤＥＳ（Ｋｓｔｍ，ＣＫ）と表記される。この一実施形態では、暗号化した値は、５６ビットにエラー検出用のＣＲＣ（８ビット）を加えた６４ビット長でもって扱われる。

【００４９】コンテンツのトラック内にパーツデータエリア１０２が規定され、パーツキーＰＫがパーツ毎に記録される。パーツは、１６Ｋバイトのブロック１０３の集合であり、各ブロックには、ブロックシードＢＫ_ＳＥＥＤ、イニシャルベクターＩＮＶが記録されている。パーツキーＰＫは、コンテンツを暗号化するブロックキーＢＫを作成するために、コンテンツキーＣＫとペアで使用されるものである。すなわち、ＢＫ＝ＤＥＳ（ＣＫ（＋）ＰＫ，ＢＫ_ＳＥＥＤ）（５６ビット＋８ビット）である。（＋）は、排他的論理和を表す。イニシャルベクターＩＮＶは、ブロックの暗号化、復号化の初期値である。

【００５０】図８Ｂは、レコーダ１内におけるコンテンツを示す。キーエリア１１１にコンテンツ毎のコンテンツキーＣＫが復号化され、レコーダ１に固有のストレージキーＫｓｔｄで再暗号化されて保持される。すなわち、復号化は、ＩＤＥＳ（Ｋｓｔｍ，ＣＫ）（５６ビット＋８ビット）と表記され、再暗号化は、ＤＥＳ（Ｋｓｔｄ，ＣＫ）（５６ビット＋８ビット）表記される。コンテンツを構成するパーツデータエリア１１２毎にブロックキーＢＫを作成するためのパーツキーＰＫが記録される。パーツを構成するブロック１１３のそれぞれには、ブロックシードＢＫ_ＳＥＥＤ、イニシャルベクターＩＮＶが記録されている。メモリカード上と同様に、ブロックキーＢＫは、ＢＫ＝ＤＥＳ（ＣＫ（＋）ＰＫ，ＢＫ_ＳＥＥＤ）（５６ビット＋８ビット）である。

【００５１】図９は、録音時の暗号化の処理の流れを説明するために、簡略化したブロック図であり、図１と対応する部分には、同一符号を付して示し、暗号化の説明に特に不要な構成は、省略されている。Ｓｅｋは、認証成立時にレコーダ１とメモリカード４０との間で共有されるセッションキーである。また、ディジタルオーディオ入力１０のソースとしてＣＤ１０'が示されている。

【００５２】メモリカード４０がレコーダ１に装着されると、装着したメモリカードがセキュリティ対応のものかどうかがブート領域中の識別情報によって決定される。セキュリティ対応のものと決定されると、レコーダ１とメモリカード４０との間で、相互に正規のものであるかを認証する。

【００５３】図１０は、認証時のセット（レコーダ１）およびメモリカード４０間の暗号化の処理を示すものである。最初のステップＳ１において、メモリカード４０のセキュリティブロック５２内の乱数発生器によって乱数Ｒｍを発生し、メモリカード４０のシリアル番号ＩＤと共に送信する。

【００５４】レコーダ１では、ステップＳ２の処理を行う。すなわち、ＲｍとＩＤとを受け取り、ＩＫｊ＝ＭＡＣ（ＭＫｊ，ＩＤ）の関係にしたがって、認証キーＩＫｊを生成する。ＭＫｊは、レコーダ１のセキュリティブロック３に記憶されている複数のマスターキーMK_0～MK_{31}の内で選択された一つのマスターキーである。レコーダ１は、乱数Ｒｄを発生し、認証キーでメッセージ認証子MAC_A（Message Authentication Code）、すなわち、ＭＡＣ（ＩＫｊ，ＩＤ//Ｒｍ//Ｒｄ）を作成する。ここで、Ａ//Ｂは、ＡとＢの連結（ｎビットのＡの後ろにｍビットのＢを結合して（ｎ＋ｍ）ビットとしたもの）を示す。そして、レコーダ１が乱数Ｓｄを発生し、Ｒｄ//Ｓｄ//MAC_A //ｊをメモリカード４０へ送信する。

【００５５】メモリカード４０は、ステップＳ３において、このデータＲｄ//Ｓｄ//MAC_A //ｊを受け取り、ｊからセキュリティブロック５２内の認証キーＩＫｊを見つけ、認証キーＩＫｊおよびＲｄ、Ｒｍ、ＩＤを用いてMAC_Bを計算する。計算したMAC_Bが受け取ったMAC_Aと同一であれば、メモリカード４０は、正しいとしてセット（レコーダ）を認める。そして、ステップＳ４において、メモリカード４０は、MAC_C＝ＭＡＣ（ＩＫｊ，Ｒｍ//Ｒｄ）を作成し、乱数Ｓｍを発生する。その後、メモリカード４０は、Ｓｍ//MAC_Cをレコーダ１に送信する。

【００５６】ステップＳ５において、レコーダ１は、Ｓｍ//MAC_Cを受け取る。レコーダ１は、ＩＫｊ，Ｒｍ，Ｒｄを用いてMAC_Dを計算する。計算したMAC_Dが受け取ったMAC_Cと同一であれば、レコーダ１は、正しいとしてメモリカード４０を認める（すなわち、認証する）。この段階では、レコーダ１およびメモリカード４０の両者が選択した認証キーＩＫｊおよび乱数Ｓｄ、Ｓｍを有している。そして、レコーダ１は、ステップＳ６において、ＭＡＣ（ＩＫｊ，Ｒｍ//Ｒｄ）をセッションキーＳｅｋと指定する。メモリカード４０側でも、ＭＡＣ（ＩＫｊ，Ｒｍ//Ｒｄ）をセッションキーＳｅｋと指定する。このように、正しく相互認証がなされると、セッションキーＳｅｋをレコーダ１とメモリカード４０とが共有する。セッションキーは、認証が成立する度に生成される。

【００５７】図１１は、レコーダ１によりオーディオファイルをメモリカード４０のフラッシュメモリ４２に記

録する時のキーの書き込み処理を示す。なお、書き込み処理を開始するときには、セッションキーＳｅｋの生成処理が終了しており、セッションキーＳｅｋをレコーダ１とメモリカード４０とが共有している。ステップＳ１１において、レコーダ１は、コンテンツのトラックデータ毎に乱数を発生し、乱数に応じてたコンテンツキーＣＫを作成する。次に、ステップＳ１２において、レコーダ１は、コンテンツキーＣＫをセッションキーＳｅｋで暗号化し、暗号化したＤＥＳ（Ｓｅｋ，ＣＫ）をメモリカード４０に送信する。

【００５８】メモリカード４０は、ステップＳ１３において、このデータを受け取り、セッションキーでコンテンツキーＣＫを復号する。すなわち、ＩＤＥＳ（Ｓｅｋ，ＤＥＳ（Ｓｅｋ，ＣＫ））と復号処理が表記される。次のステップＳ１４において、メモリカード４０は、復号したコンテンツキーＣＫをメモリカード４０のストレージキーＫｓｔｍで再度、暗号化し、再暗号化したコンテンツキーＤＥＳ（Ｋｓｔｍ，ＣＫ）がレコーダ１に送信される。

【００５９】レコーダ１は、ステップＳ１５において、再暗号化したコンテンツキーを、パーツデータエリア１１２を管理するキーエリア１１１に配置させ、再暗号化されたコンテンツキーＣＫおよびコンテンツがメモリカード４０のフラッシュメモリに記録されるようにフォーマット化の処理を行う。コンテンツの暗号化のために、図９に示されるように、コンテンツキーＣＫとパーツキーＰＫとの排他的論理和または論理積がとられる。その結果、テンポラリーキーＴＭＫが得られる。テンポラリーキーＴＭＫは、セキュリティブロック３内にのみ存在し、外部からはアクセス可能ではない。各ブロック１１３の先頭で乱数を発生し、これをブロックシードＢＫ_ＳＥＥＤとし、各パーツデータエリア１１２内に格納される。レコーダ１は、テンポラリーキーＴＭＫでブロックシードＢＫ_ＳＥＥＤを暗号化し、ブロックキーＢＫが得られる。すなわち、ＢＫ＝（ＣＫ（＋）ＰＫ，ＢＫ_ＳＥＥＤ）の関係が得られる。ブロックキーＢＫもセキュリティブロック３内にのみ存在し、セキュリティブロック３の外部からはアクセス可能ではない。

【００６０】ステップＳ１６において、レコーダ１は、ブロックキーＢＫによってパーツデータエリア１１２内のデータをブロック毎に暗号化し、暗号化されたデータと、キーエリア１１１内のデータをメモリカード４０に送信する。メモリカード４０は、レコーダ１から受け取った暗号化されたデータおよびキーエリア１１１内のデータ（ヘッダデータ）をフラッシュメモリ４２に記録する（ステップＳ１７）。

【００６１】図１２は、レコーダ１がメモリカード４０のフラッシュメモリ４２に蓄えられているオーディオトラックを再生する時の処理の流れを説明するために、簡略化したブロック図であり、図１と対応する部分には、同一符号を付して示し、暗号化および復号化の説明に特に不要な構成は、省略されている。図１３は、図１２と同様に、レコーダ１によりオーディオトラックをメモリカード４０のフラッシュメモリ４２から再生する時の復号化処理を示す。再生時でも、相互認証が成立することによって、レコーダ１とメモリカード４０との間でセッションキーＳｅｋが共有される。

【００６２】ステップＳ２１において、レコーダ１は、メモリカード４０からデータ読み出すことによって、ストレージキーＫｓｔｍで暗号化されたコンテンツキーＣＫすなわち、（ＤＥＳ（Ｋｓｔｍ，ＣＫ））と、暗号化されたコンテンツ（所望のトラックのパーツデータエリア１０２）を得る。そして、レコーダ１は、ストレージキーＫｓｔｍで暗号化されたコンテンツキーＣＫをメモリカード４０に渡す。

【００６３】ステップＳ２２において、メモリカード４０は、ストレージキーＫｓｔｍでコンテンツキーＣＫを復号する（ＩＤＥＳ（Ｋｓｔｍ，ＤＥＳ（Ｋｓｔｍ，ＣＫ））。ステップＳ２３において、メモリカード４０は、復号したコンテンツキーをセッションキーＳｅｋで暗号化し、ＤＥＳ（Ｓｅｋ，ＣＫ）をレコーダ１に送る。

【００６４】レコーダ１は、ステップＳ２４において、セッションキーＳｅｋでコンテンツキーを復号する。次のステップＳ２５において、レコーダ１は、復号したコンテンツキーＣＫと、パーツキーＰＫと、ブロックシードＢＫ_ＳＥＥＤを使用してブロックキーＢＫを作成する。ステップＳ２６では、レコーダ１は、ブロック毎にブロックキーＢＫによって暗号化されたパーツデータエリア１０２をそれぞれ復号化する。復号化されたオーディオデータがオーディオエンコーダ／デコーダ７によって復号化される。

【００６５】上述した読み出し動作、書き込み動作以外においても、状態１において、コマンドが伝送され、その後の状態２において、コマンドに対応するデータが伝送される。レコーダ１とメモリカード４０間のシリアルインタフェースは、上述したものに限定されず、種々のものを使用できる。

【００６６】この発明の一実施形態におけるレコーダ１とメモリカード４０との間のシリアンインタフェースについてより詳細に説明する。図２に示されるように、レコーダ１とメモリカード４０との間を結合する１０本の線の内で、信号の送受信にとって主要なものは、クロック線ＳＣＫ、ステータス線ＳＢＳおよびデータ線ＤＩＯである。

【００６７】図１４は、メモリカード４０からデータを読み出す時のタイミングを示す。状態０（初期状態）以外の状態において、クロック線ＳＣＫを介して伝送されるデータと同期したクロックが伝送される。レコーダ１とメモリカード４０との間で、何等データの送受信がさ

れていない状態では、ステータス線ＳＢＳがローレベルとなっている。これが状態０（初期状態）である。そして、タイミングｔ31において、レコーダ１がステータス線ＳＢＳをハイレベルとし、状態１となる。

【００６８】メモリカード４０（Ｓ／Ｐ，Ｐ／Ｓ，ＩＦブロック４３）は、ステータス線ＳＢＳがハイレベルに切り替わったことによって、状態０から状態１へ変化したことを検出する。状態１では、データ線ＤＩＯを介してレコーダ１からメモリカード４０に対して読み出しコマンドが送信され、メモリカード４０が読み出しコマンドを受信する。この読み出しコマンドは、シリアルインタフェース用のＴＰＣ(Serial Protocol Command) と称されるプロトコルコマンドである。後述するように、プロトコルコマンドによって、通信の内容と後続するデータのデータ長が特定される。

【００６９】コマンドの送信が完了したタイミングｔ32において、ステータス線ＳＢＳがハイレベルからローレベルに切り替えられる。それによって、状態１から状態２へ遷移する。状態２では、メモリカード４０が受信したコマンドで指示される処理、具体的には、読み出しコマンドで指定されたアドレスのデータをフラッシュメモリ４２から読み出す処理を行う。この処理がなされている間、データ線ＤＩＯを介してビジー信号（ハイレベル）がレコーダ１に送信される。

【００７０】そして、フラッシュメモリ４２からデータの読み出しが完了したタイミングｔ33において、ビジー信号の出力が停止され、レコーダ１に対してメモリカード４０からデータを送出する準備ができたことを示すレディー信号（ローレベル）の出力が開始される。

【００７１】レコーダ１は、メモリカード４０からレディー信号を受信することによって、読み出しコマンドに対応する処理が準備できたことを知り、タイミングｔ34において、ステータス線ＳＢＳをハイレベルに切り替える。すなわち、状態２から状態３へ遷移する。

【００７２】状態３になると、メモリカード４０は、状態２においてページバッファ４５に読み出したデータをデータ線ＤＩＯを介してレコーダ１に対して出力する。読み出しデータの転送が完了したタイミングｔ35において、レコーダ１は、クロック線ＳＣＫを介して伝送されていたクロックの供給を停止すると共に、ステータス線をハイレベルからローレベルへ切り替える。それによって、状態３から初期状態（状態０）に遷移する。

【００７３】なお、メモリカード４０の内部状態に変化が生じて何らかの割り込み処理を行う必要が発生すると、メモリカード４０は、タイミングｔ36で示すように、状態０において、割り込みを示すインターラプト信号をデータ線ＤＩＯを介してレコーダ１に供給する。レコーダ１は、状態０でメモリカード４０からデータ線ＤＩＯを介して信号が供給された場合、その信号がインターラプト信号であることを認識できるように設定されている。レコーダ１がインターラプト信号を受け取ると、そのインターラプト信号に基づいて必要な処理を行う。

【００７４】図１５は、メモリカード４０のフラッシュメモリ４２に対してデータを書き込む時のタイミングチャートである。初期状態（状態０）では、クロックＳＣＫの伝送がされない。タイミングｔ41において、レコーダ１がステータス線ＳＢＳをローレベルからハイレベルに切り替える。それによって、データ線ＤＩＯを介して書き込みコマンドが伝送される状態１に遷移する。メモリカード４０は、状態１において、コマンドを取得するように準備する。タイミングｔ41からコマンドがデータ線ＤＩＯを介してメモリカード４０に伝送され、メモリカード４０がこの書き込みコマンドを取得する。

【００７５】書き込みコマンドの送信が完了したタイミングｔ42において、レコーダ１がステータス線ＳＢＳをハイレベルからローレベルに切り替える。それによって、状態１から状態２へ遷移する。状態２では、レコーダ１が書き込みデータをデータ線ＤＩＯを介してメモリカード４０に伝送する。メモリカード４０では、受け取った書き込みデータがページバッファ４５に蓄えられる。

【００７６】書き込みデータの伝送が終了するタイミングｔ43において、ステータス線ＳＢＳがローレベルからハイレベルへ切り替えられ、状態２から状態３へ遷移する。状態３において、メモリカード４０は、書き込みデータをフラッシュメモリ４２へ書き込む処理を行う。状態３において、メモリカード４０は、データ線ＳＢＳを介してビジー信号（ハイレベル）をレコーダ１に対して送信する。レコーダ１は、書き込みコマンドを送信し、且つ現在の状態が状態３であることから、メモリカード４０から送信される信号がステータス信号であると判断する。

【００７７】メモリカード４０において、書き込みデータの書き込み処理が終了すると、終了したタイミングｔ44において、ビジー信号の出力を停止し、レディー信号（ローレベル）をレコーダ１に対して送信する。レコーダ１は、レディー信号を受信すると、書き込みコマンドに対応する書き込み処理が完了したものと判断し、クロック信号の送信を止めると共に、タイミングｔ45においてステータス線ＳＢＳをハイレベルからローレベルへ切り替える。それによって、状態３から状態０（初期状態）に戻る。

【００７８】さらに、状態０において、メモリカード４０からデータ線ＤＩＯを介してハイレベルの信号をレコーダ１が受け取った場合には、レコーダ１がこの信号をインターラプト信号と認識する。そして、レコーダ１は、受信したインターラプト信号に基づいて必要な処理を行う。例えばメモリカード４０をレコーダ１から取り外した時に、メモリカード４０がインターラプト信号を発生する。

【００７９】上述した読み出し動作、書き込み動作以外においても、状態１において、コマンドが伝送され、その後の状態２において、コマンドに対応するデータが伝送される。レコーダ１とメモリカード４０間のシリアルインタフェースは、上述したものに限定されず、種々のものを使用できる。

【００８０】この発明の一実施形態において、メモリカードを使用できる機器によりなされる処理について図１６を参照してより詳細に説明する。機器の電源がオンされると（ステップＳ２００）、ステップＳ２０１でメモリカードが挿入されているかどうかが決定される。メモリカードが挿入されていると決定されると、メモリカードのブートブロックが読み込まれる（ステップＳ２０２）。

【００８１】図７を参照して説明したように、ブートブロックのブート＆アトリビュート情報中には、セキュリティ対応かどうかの識別情報が含まれている。この識別情報を参照して、挿入されたメモリカードがセキュリティ対応か、非対応かが決定される（ステップＳ２０３）。セキュリティ対応のメモリカード４０であれば、ステップＳ２０４において、認証動作がなされ、認証成立後にコンテンツデータの記録／再生がなされる（ステップＳ２０５）。

【００８２】ステップＳ２０３において、挿入されたメモリカードがセキュリティ非対応のメモリカード４０'であると決定されると、ステップＳ２０６において、挿入したメモリカード４０'が使用できない旨の告知がなされる。表示デバイス５上で警告メッセージを表示することによって、告知がなされる。音声等の他の方法によって告知を行っても良い。

【００８３】上述した処理は、レコーダ１のように、セキュリティ対応の機器が行うものである。若し、機器がセキュリティ非対応の場合には、図１６において破線で示すように、ステップＳ２０２（ブートブロックの読み込み）の後に、ステップＳ２０７に処理が移る。ステップＳ２０７では、挿入されたメモリカードがセキュリティ対応か、非対応かが決定される。ステップＳ２０７における決定の結果が肯定、否定の何れであっても、ステップＳ２０８およびＳ２０９で示すように、メモリカード４０'に対して、通常動作（書き込み、読み出し、消去等）を行うことができる。

【００８４】以上説明した一実施形態では、メモリカードの機能がセキュリティ機能であってたが、この発明は、セキュリティ機能に限定されるものではない。例えば機器とメモリカードとのインタフェースにおける通信速度またはデータレートが既存の速度（低速）より速い速度（高速）が可能とされる。この速度に関しての新機能をメモリカードが持つ場合に対して、この発明を適用できる。

【００８５】図１７は、速度に関する処理を示すフローチャートである。ステップＳ３００で電源がオンされ、ステップＳ３０１でメモリカードが挿入されたかどうかが決定され、ステップＳ３０２でブートブロックが読み込まれる。ブロックブロック中には、セキュリティ機能と同様に、そのメモリカードが高速対応か、非対応かの識別情報が含まれている。

【００８６】この識別情報によって、メモリカードが高速対応と決定すれば、機器とメモリカード間の通信速度またはデータレートを低速から高速へ切り替え（ステップＳ３０４）、高速動作がなされる（ステップＳ３０５）。若し、ステップＳ３０３において、高速非対応と決定されると、低速動作がなされる（ステップＳ３０６）。機器が高速非対応の場合には、図１７において破線で示すように、高速対応かどうかの決定（ステップＳ３０７）の結果に影響されずに、低速動作がなされる（ステップＳ３０８およびＳ３０９）。

【００８７】なお、上述した説明では、ＤＥＳを使用した場合を説明したが、セキュリティのための方式としては、ＤＥＳに限らず、種々の暗号化技術を採用することが多能である。

【００８８】

【発明の効果】この発明によれば、メモリカードのように着脱自在のメモリ装置として、新機能を有するものと、それを有しないものとが混在していても、装着時に新機能の有無を機器が瞬時に決定することができる。従って、実際に機器がメモリカードと通信を行ってエラーとなるかどうかによって、新機能の有無を決定する方法と異なり、無駄な動作を生じることがない。また、メモリ装置の形状によって、新機能の有無を識別する方法と異なり、新機能を有するメモリカードを新機能に対応していない機器によって使用することが可能となり、メモリカードの互換性の点で有利である。

【図面の簡単な説明】

【図１】この発明の一実施形態の全体的構成を示すブロック図である。

【図２】この発明の一実施形態におけるセキュリティ対応のメモリカードの構成を示すブロック図である。

【図３】この発明の一実施形態におけるセキュリティ非対応のメモリカードの構成を示すブロック図である。

【図４】この発明の一実施形態におけるフラッシュメモリのファイルシステム処理階層の構成を示す略線図である。

【図５】この発明の一実施形態におけるフラッシュメモリのデータの物理的構成のフォーマットを示す略線図である。

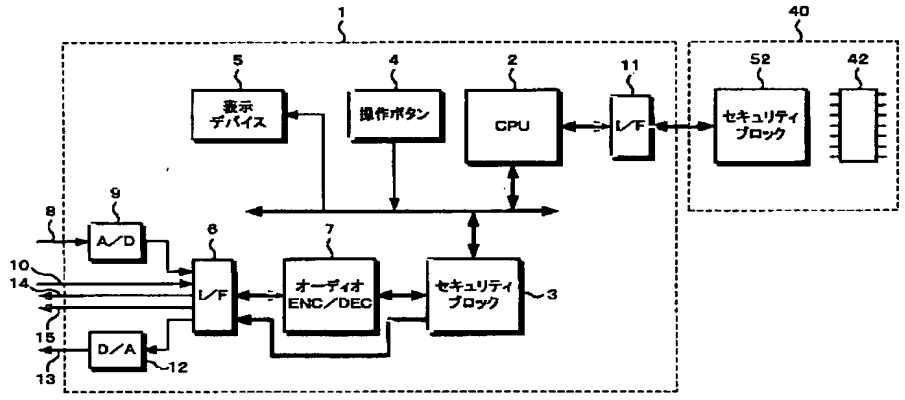
【図６】フラッシュメモリのブートブロックの構成を示す略線図である。

【図７】フラッシュメモリのブートブロックのブートおよびアトリビュート情報の構成を示す略線図である。

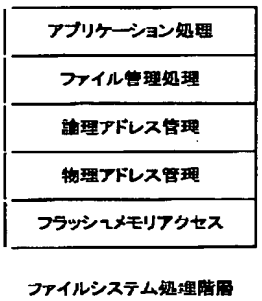
【図８】この発明の一実施形態におけるコンテンツにお

けるキーの関係を示す略線図である。
【図９】この発明の一実施形態における録音時の暗号化処理を説明するためのブロック図である。
【図１０】この発明の一実施形態における認証処理を説明するための略線図である。
【図１１】この発明の一実施形態における録音時の暗号化処理を説明するための略線図である。
【図１２】この発明の一実施形態における再生時の暗号化処理を説明するためのブロック図である。
【図１３】この発明の一実施形態における再生時の暗号化処理を説明するための略線図である。
【図１４】この発明の一実施形態におけるレコーダとメモリカード間のインタフェースを説明するためのタイミングチャートである。
【図１５】この発明の一実施形態におけるレコーダとメモリカード間のインタフェースを説明するためのタイミングチャートである。
【図１６】この発明の一実施形態の動作説明に用いるフローチャートである。
【図１７】この発明をセキュリティ機能以外の機能に対して適用した例を説明するためのフローチャートである。
【符号の説明】
１・・・レコーダ、２・・・ＣＰＵ、３・・・セキュリティブロック、７・・・オーディオエンコーダ／デコーダ、１１・・・メモリインタフェース、４０・・・セキュリティ対応のメモリカード、４０’・・・セキュリティ非対応のメモリカード、４３・・・Ｓ／Ｐ，Ｐ／Ｓ，ＩＦブロック、４２・・・フラッシュメモリ、５２・・・セキュリティブロック

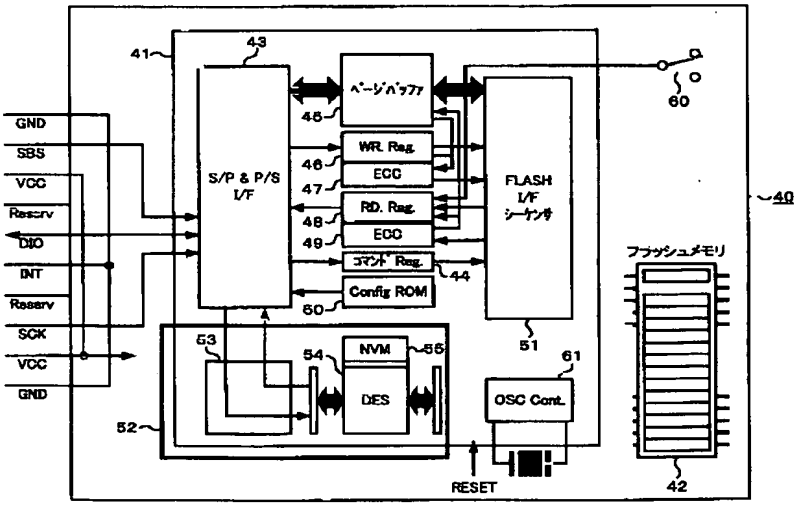
【図１】



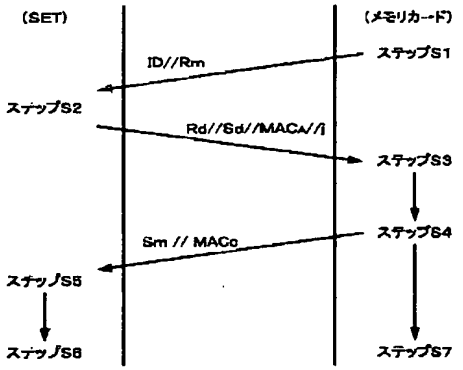
【図４】



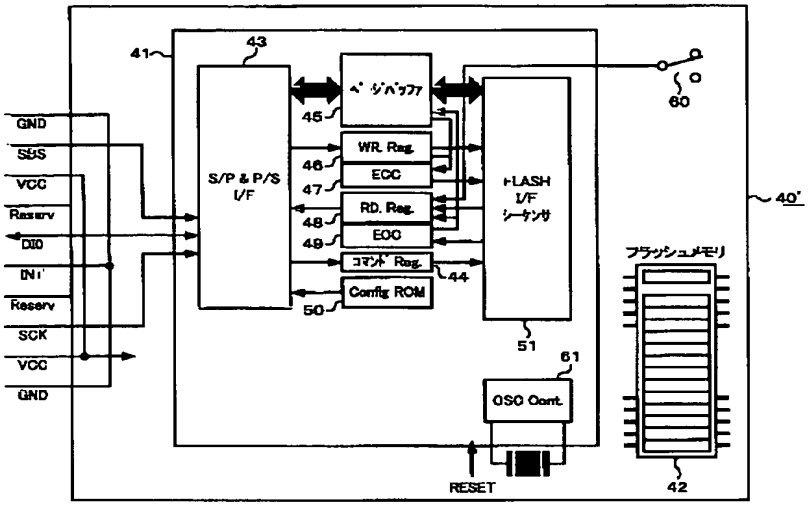
【図２】



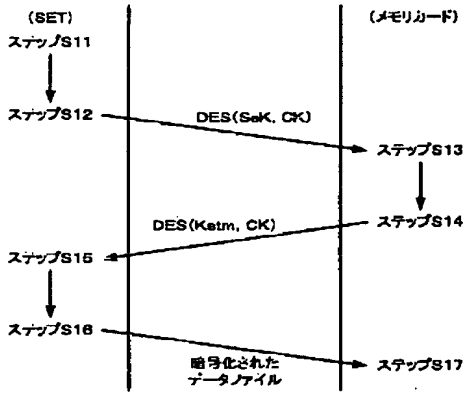
【図１０】



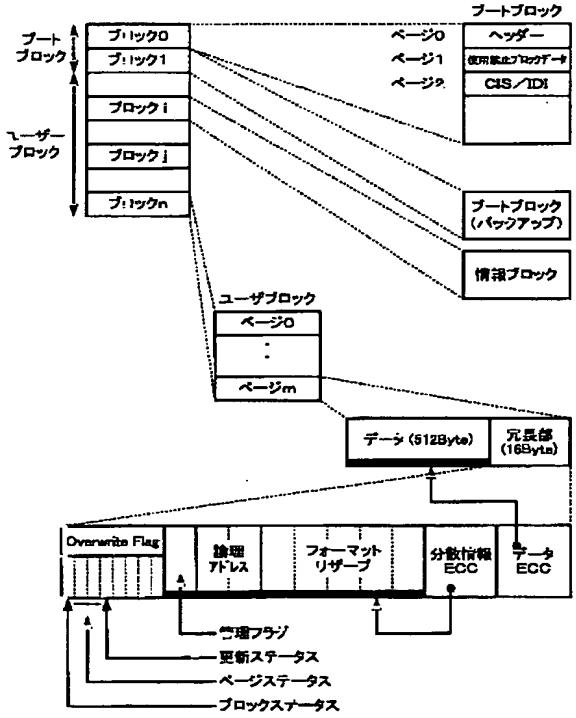
【図3】


41
43
45
46
47
48
49
50
51
60
61
40'
42
44
GND
SBS
VCC
Reserv
DIO
INT
Reserv
SCK
VCC
GND
S/P & P/S I/F
WR. Reg.
ECC
RD. Reg.
ECC
Config ROM
FLASH I/F シーケンサ
OSC Cont.
RESET
フラッシュメモリ

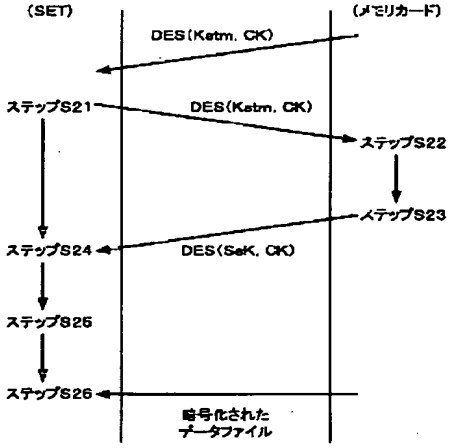
【図11】


(SET)
(メモリカード)
ステップS11
ステップS12
DES(SeK, CK)
ステップS13
DES(Kstm, CK)
ステップS14
ステップS15
ステップS16
暗号化された データファイル
ステップS17

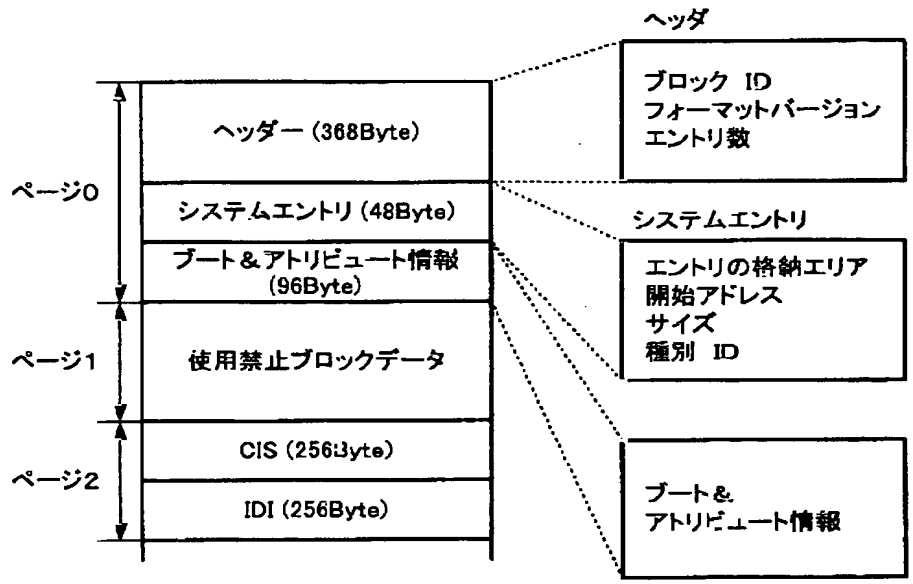
【図5】


ブートブロック
ユーザーブロック
ブロック0
ブロック1
ブロックi
ブロックj
ブロックn
ページ0
ページ1
ページ2
ヘッダー
CIS/IDI
ブートブロック (バックアップ)
情報ブロック
ユーザブロック
ページ0
ページm
データ (512Byte)
冗長部 (16Byte)
Overwrite Flag
論理アドレス
フォーマットリザーブ
分散情報ECC
データECC
管理フラグ
更新ステータス
ページステータス
ブロックステータス

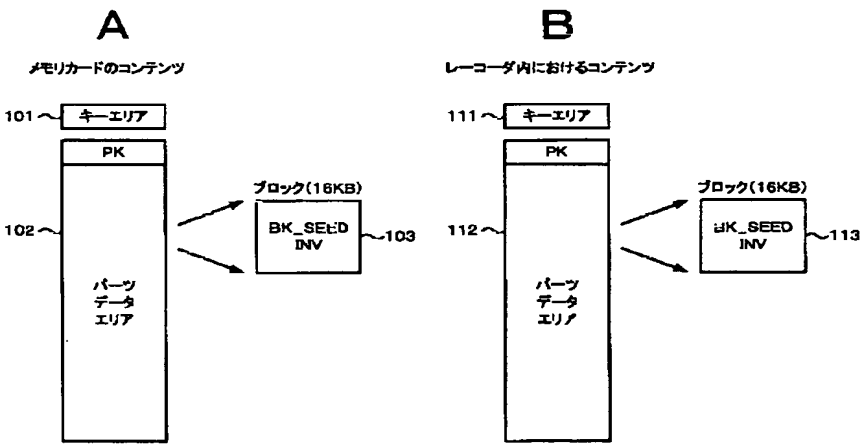
【図13】


(SET)
(メモリカード)
DES(Kstm, CK)
ステップS21
DES(Kstm, CK)
ステップS22
ステップS23
ステップS24
DES(SeK, CK)
ステップS25
ステップS26
暗号化された データファイル

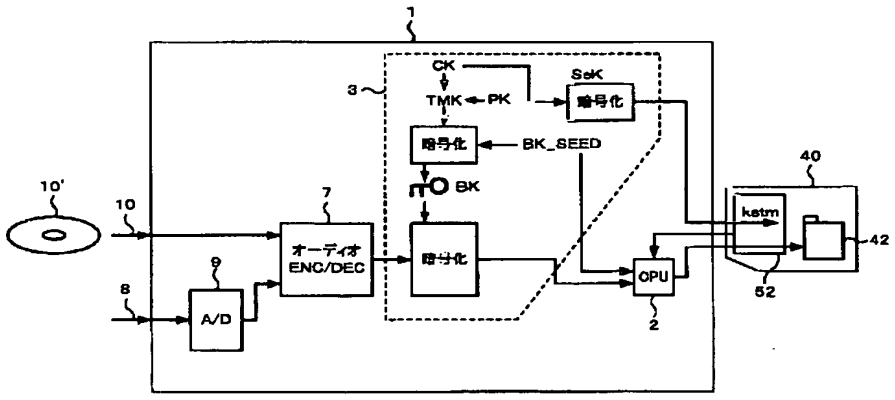
【図6】


ヘッダ
ブロック ID
フォーマットバージョン
エントリ数
ヘッダー (368Byte)
システムエントリ (48Byte)
ブート&アトリビュート情報 (96Byte)
ページ0
システムエントリ
エントリの格納エリア
開始アドレス
サイズ
種別 ID
ページ1
使用禁止ブロックデータ
CIS (256Byte)
ページ2
IDI (256Byte)
ブート&
アトリビュート情報

【図8】


A
メモリカードのコンテンツ
101
キーエリア
PK
102
パーツ
データ
エリア
ブロック(16KB)
BK_SEED
INV
103
B
レーコーダ内におけるコンテンツ
111
キーエリア
PK
112
パーツ
データ
エリア
ブロック(16KB)
BK_SEED
INV
113

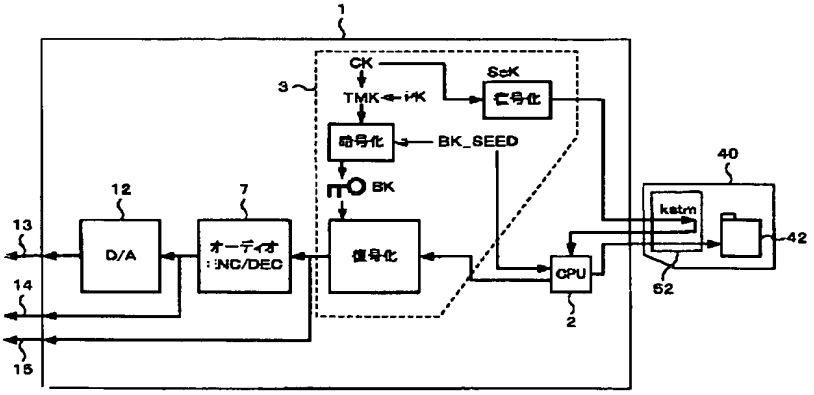
【図9】


1
3
CK
SeK
TMK
PK
暗号化
暗号化
BK_SEED
BK
40
10'
10
7
オーディオ
ENC/DEC
暗号化
kstm
42
9
8
A/D
OPU
2
52

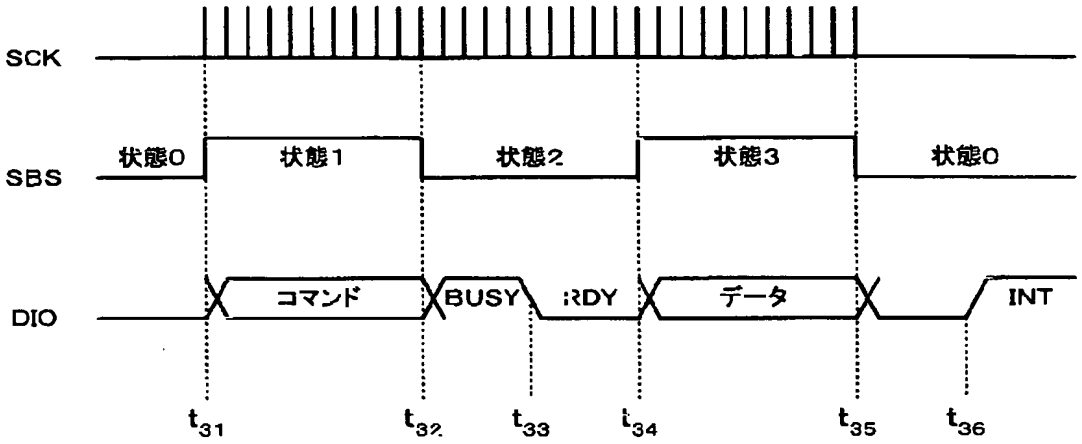
【図7】

		バイト数	
MS クラス	(*1)	1	1:Type-1 Other reserved
カードタイプ	(*1)	1	1:Read Only 2:Read Write 3:Hybrid Other reserved
ブロックサイズ	(*1)	2	KB単位でブロックサイズを表現 16KB:0x0010 8KB:0x0008
ブロック数	(*1)	2	ブロック数
総ブロック数	(*1)	2	総ブロックの数
ページサイズ		2	ページサイズ512固定0x0200
冗長部サイズ		1	冗長部サイズ16バイトの場合0x10
セキュリティ対応	(*1)	1	
アセンブリ日時	(*2)	8	カード(ハード)の作成年月日 (次ページ日時指定フォーマット参照)
事業所エリア	(*2)	4	シリアル番号等の事業所管理に使用
MS アセンブリメーカーコード	(*2)	1	登録のアセンブリメーカーコード
MS アセンブリ機種コード	(*2)	3	登録のアセンブリ機種コード
メモリメーカーコード		2	チップのメーカーコード 0:不明
メモリデバイスコード		2	デバイスコード 0:不明
メモリサイズ		2	MByte数を記述ex) 32Mbit Flash 0x0004
フォーマットリザーブ		1	1を設定 Other reserved
フォーマットリザーブ		1	1を設定 Other reserved
VCC		1	VCC単位0.1Vで表現ex) 3.3V 0x21
VPP		1	VPP単位0.1Vで表現ex) 3.3V 0x21
コントローラ番号		2	コントローラチップ番号
リザーブ		14	
フォーマット種別	(*1)	1	1:FAT Other reserved
用途		1	0:汎用 Other reserved
ゼロリセットリザーブ		5	
リザーブ		35	

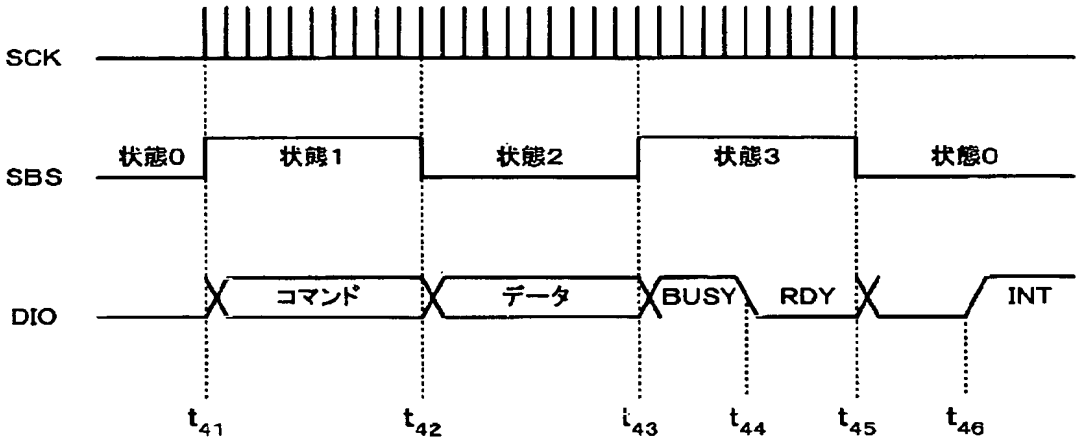
【図12】



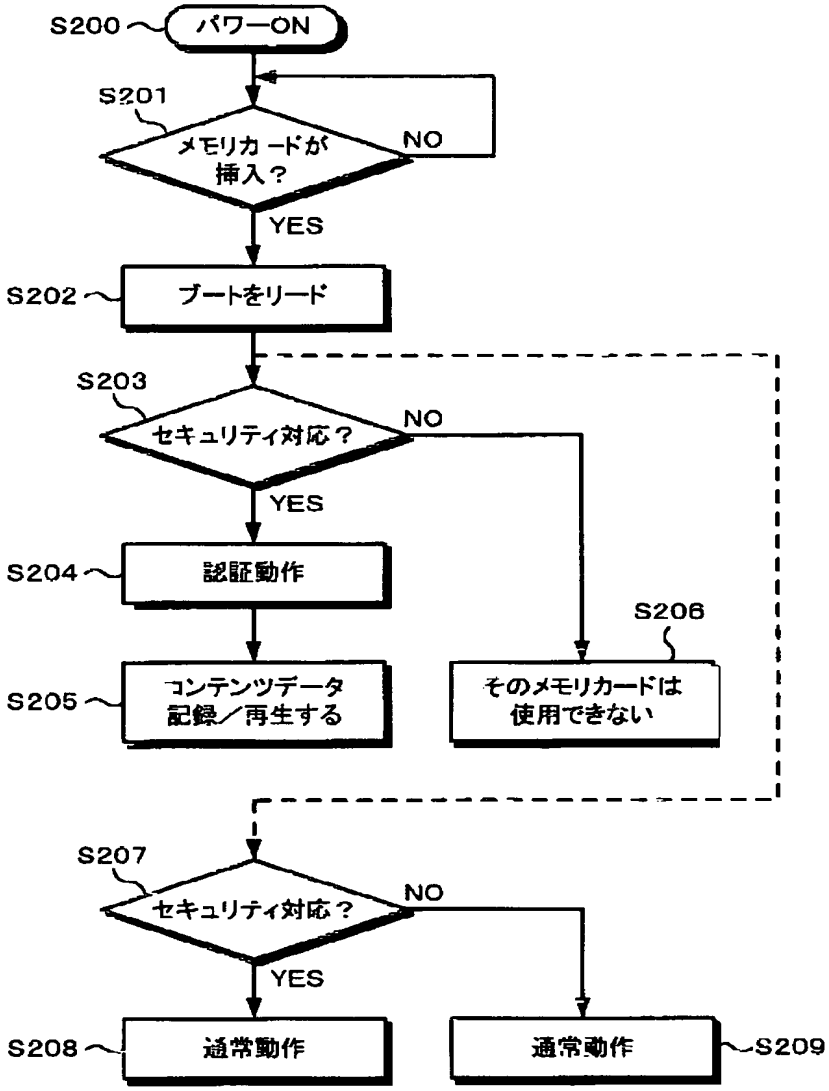
【図14】


SCK
SBS
DIO
状態0
状態1
状態2
状態3
状態0
コマンド
BUSY
RDY
データ
INT
t_{31}
t_{32}
t_{33}
t_{34}
t_{35}
t_{36}

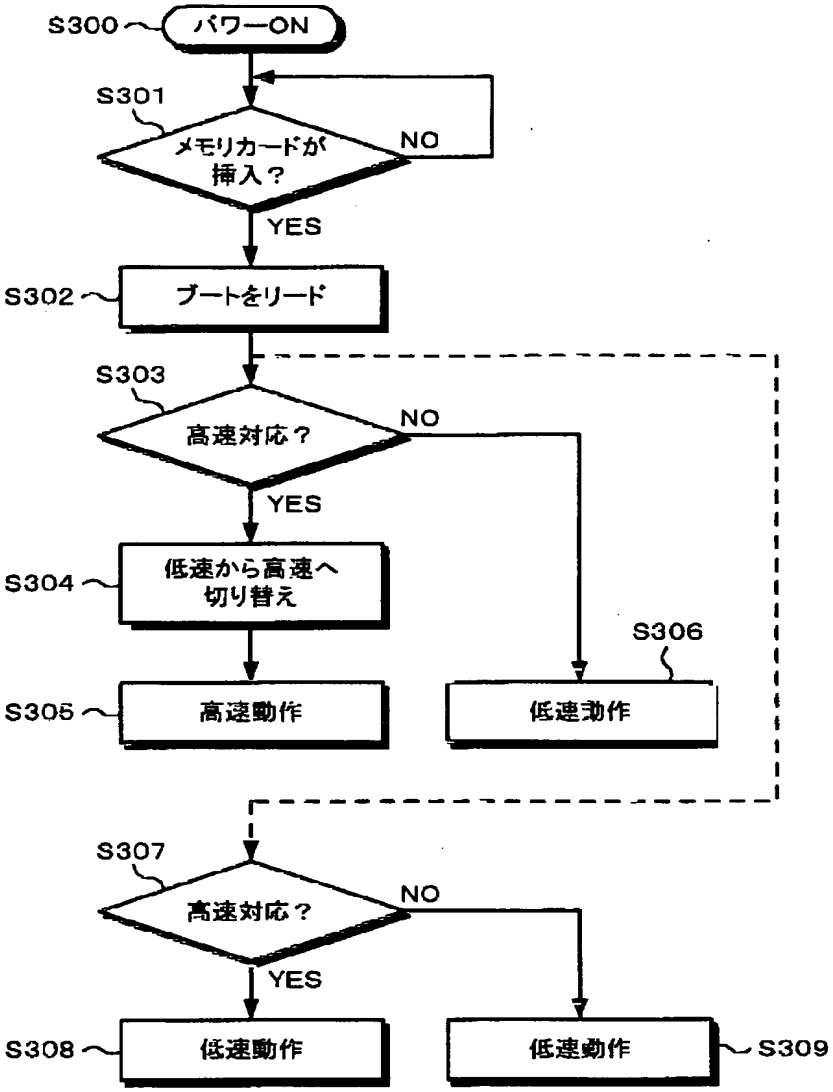
【図15】


SCK
SBS
DIO
状態0
状態1
状態2
状態3
状態0
コマンド
データ
BUSY
RDY
INT
t_{41}
t_{42}
t_{43}
t_{44}
t_{45}
t_{46}

【図16】


S200
パワーON
S201
メモリカードが挿入？
NO
YES
S202
ブートをリード
S203
セキュリティ対応？
NO
YES
S204
認証動作
S205
コンテンツデータ記録／再生する
S206
そのメモリカードは使用できない
S207
セキュリティ対応？
NO
YES
S208
通常動作
通常動作
S209

【図17】



フロントページの続き

(51)Int.Cl.[7]	識別記号	FI		(参考)
H04L 9/10		G10L 9/18	J	
		H04L 9/00	621A	

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☑ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.